UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI
CENTRAL DIVISION
(*Electronically Filed*)

MILDRED BALDWIN and DOUGLAS DYRSSEN SR., on behalf of themselves and others similarly situated, *Plaintiffs*, **v.** NATIONAL WESTERN LIFE INSURANCE COMPANY, *Defendant*,	)	Case No.: 2:21-cv-04066-WJE

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Mildred Baldwin and Douglas Dyrssen Sr. ("Plaintiffs"), on behalf of themselves and the proposed classes defined below, by undersigned counsel, allege as follows:

NATURE OF THE ACTION

1. Defendant National Western Life Insurance Company ("Defendant" or "NWL") is a life-insurance company which, according to its website, offers a broad range of life insurance and annuity products and services.

2. On or about August 15, 2020, NWL discovered that an unauthorized person had gained access to NWL's computer systems (the "Data Breach"). The unauthorized person stole 656 gigabytes worth of confidential and protected personally identifiable information ("PII"), which included the PII of NWL's former and current policyholders.

3. Within days of the Data Breach, the unauthorized person began publishing the leaked PII online. In the first of a series of posts, the unauthorized person published a screen shot

of what appears to be a file containing Data Breach victims' credit card information. A few days later, on or about August 23, 2020, the unauthorized person posted screenshots of policyholders' Social Security numbers, dates of birth, full names, dates of death, addresses, policy numbers, and policy termination dates.

4. Instead of notifying victims of the Data Breach promptly, NWL waited almost 4 months—until December 21, 2020—to start notifying policyholders and former independent agents like Plaintiff Dyrssen of the Breach.

5. According to NWL, the delay in notifying Data Breach victims was because the company was undergoing an investigation.

6. At best, NWL should have known that its policyholders' PII was being publicly disseminated on the internet. At worst, NWL, upon information or belief, knew the severity of the Data Breach but chose to ignore and downplay the ongoing public disclosure of the Data Breach victims' PII.

7. Plaintiffs each received a form notification letter dated January 25, 2021 (the "Notice Letter"), nearly five months after the Data Breach. The form letter notified Plaintiffs that "On August 15, 2020, NWL discovered a malware incident impacting certain company systems" and that "On December 21, 2020 we confirmed that personal information related to you was included in the impacted data."

8. The Notice Letter did not warn Plaintiffs that the unauthorized accessor was publicly disclosing Data Breach victims' PII in a series of online posts. Upon information and belief, NWL was attempting to downplay the Data Breach's impact and severity.

9. Plaintiffs and members of the proposed classes are victims of Defendant's negligence and deceptive trade practices. Specifically, Plaintiffs and members of the proposed

classes trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices in order to prevent the Data Breach that occurred on August 15, 2020, and when the Data Breach was discovered, Defendant attempted to downplay and minimize the impact of the Breach.

10. Defendant's negligence and deceptive practices caused real and substantial damage to Plaintiffs and members of the proposed classes.

11. Plaintiffs and members of the proposed classes therefore bring this lawsuit seeking damages and restitution for Defendant's actions.

THE PARTIES

12. Plaintiff Mildred Baldwin is a natural person and citizen of the state of Missouri, residing in Sedalia, Missouri.

13. Plaintiff Douglas Dyrssen Sr. is, and at all times mentioned herein was, an individual citizen of the State of California residing in Modesto, California. Plaintiff Dyrssen was an independent insurance agent who previously sold policies written by Defendant NWL. By letter dated January 25, 2021, Plaintiff Dyrssen received notice from Defendants that the Data Breach had occurred following an attack on Defendants' computer systems, and that his personal data was involved.

14. Defendant NWL is a Colorado corporation that maintains its principal place of business in Austin, Texas, and is a wholly owned subsidiary of National Western Life Group, Inc. At all relevant times, NWL routinely conducts and does substantial business in Missouri.

JURISDICTION AND VENUE

15. This Court has jurisdiction pursuant to 28 U.S.C. § 1441, as this case was removed to this Court after initially being filed in Missouri state court.

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and Plaintiffs and members of the proposed Class are citizens of states different from Defendant.

17. This Court has personal jurisdiction over Defendant because Defendant does substantial business in this State. Defendant is registered with the State of Missouri to sell insurance products and at all relevant times to this action, sought and solicited its insurance products in Missouri.

18. Upon information and belief, NWL recruits and trains agents to sell its life insurance products in Missouri.[1]

19. This Court also has personal jurisdiction over NWL through its business operations in this District, the specific nature of which (i.e., the sale of insurance policies and the gathering of personal information) occurs in this District. Defendants intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, and because Plaintiff Baldwin resides in this judicial district.

COMMON FACTUAL ALLEGATIONS

21. Plaintiffs and members of the proposed classes are current and former policyholders of NWL, as well as former independent agents who sold NWL policies.

[1] *See, e.g.*, https://evervest.us/wp-content/uploads/2019/07/National-Western-Product-Training.pdf (last visited February 10, 2021).

22. As a prerequisite to coverage, NWL requires purchasers of its life insurance policies and annuities to provide NWL with their PII. In its ordinary course of business, NWL maintains policyholders' full names, addresses, dates of birth, dates of death, Social Security numbers, policy numbers, policy termination dates, driver's license information and passport information.

23. Also, as a prerequisite to selling NWL policies as an independent agent, individuals (including Plaintiff Dyrssen) were required to provide NWL with their PII (including without limitation their name, address, and Social Security number), which NWL then maintains in the ordinary course of business.

24. NWL informs the purchasers of its life insurance products that NWL collects and maintains policyholders' PII through its Customer Privacy Policy (the "Privacy Policy"). NWL makes state and territory-specific Customer Privacy Policies available on its website at https://www.nationalwesternlife.com/PrivacyPolicy (last visited February 12, 2021).

25. The Privacy Policy states that "National Western Life does not disclose nonpublic personal information about you to anyone except as is necessary in order to provide our products or services to you or as required or permitted by law or as authorized by you." The Privacy Policy also states that that NWL "restrict[s] access to nonpublic personal information about you to those employees and agents who need to know that information to provide products or services to you." The Privacy Policy as it relates to Missouri, revised in March of 2002, is attached hereto as **Exhibit A.**

26. Plaintiffs and members of the proposed classes relied on NWL's representations that their PII would be secure before purchasing life insurance policies from NWL.

27. In purchasing NWL's life insurance policies, or by entering into business relationships with NWL to sell its policies, Plaintiffs and members of the proposed classes relied on NWL to keep their PII confidential and security maintained.

28. At least as of August 15, 2020, NWL discovered that the PII of its former and current policyholders and others (like Plaintiff Dyrssen) was compromised. Within days, the unauthorized accessor of NWL's computer systems publicly disclosed that it stole 656 gigabytes worth of PII from NWL's computer systems.

29. Upon information and belief, NWL failed to adequately train its employees on even the basic cybersecurity protocols, including:

a. Effective password management and encryption protocols, including, but not limited to, the use of Multi-Factor Authentication for all users;

b. Locking, encrypting and limiting access to computers and files containing sensitive information;

c. Implementing guidelines for maintaining and communicating sensitive data;

d. Protecting sensitive patient information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and

e. Providing focused cybersecurity awareness training programs for employees.

30. NWL's negligent conduct caused the Data Breach. NWL violated its obligation to implement best practices and comply with industry standards concerning computer system security. NWL failed to comply with security standards and allowed its policyholders' PII to be

stolen by failing to implement security measures that could have prevented or mitigated the Data Breach.

A. The Data Breach and Notice Letter

31. On August 15, 2020, Defendant discovered a malware incident impacting certain company computer systems.

32. Beginning on August 7, 2020, and possibly earlier, known cybercriminals gained unauthorized access to Defendant's computer systems and networks and acquired copies of Private Information held on Defendant's systems.

33. Defendant did not discover that unauthorized persons had gained access to their computer systems for over a week (from at least August 7, 2020, to August 15, 2020), and only became aware of the unauthorized access when the cyberthieves infected Defendant's IT systems with malicious software (aka malware).

34. The malware deployed "ground to a halt," Defendant's computer systems "with at least one employee reporting that there were "no systems up."[2]

35. The malware – a form of ransomware deployed by known cybercriminals (the REvil ransomware operators) also encrypted and locked out employee access to files.

36. On August 18, 2020, an independent data security research team identified a leak disclosure post on the internet, in which the REvil ransomware operators claimed to have breached Defendant's computer systems and claimed to have stolen 656 gigabytes of confidential data, consisting of 25,110 folders containing 453,695 files.

[2] https://cybleinc.com/2020/08/24/national-western-life-insurance-company-nightmare-continues/ (last accessed March 1, 2021)

37. In that same leak disclosure post, the REvil ransomware operators posted screenshots on the internet, including a snapshot of Defendant's database files, passport copies of family members of Defendant's CEO, corporate contract agreements, information about Defendant's clients, and other information.

38. On August 23, 2020, the REvil ransomware operators published another leak disclosure post online in which they claim to have access to Defendant's company emails.

39. The REvil ransomware operators also placed online and released a data archive containing approximately 1% of the total amount of data stolen.

40. Analysis of the stolen files posted by the cyberthieves in the online archive showed that the data stolen included the Private Information of Defendant's customers, including customer Social Security numbers, dates of birth, full names, dates of death, state of residence, policy numbers, and policy termination dates.

41. The cybercriminals also posted online internal NWL company emails, showing that as late as August 23, 2020, Defendants had not managed to unencrypt their encrypted files.

42. Forensic investigation later confirmed that between August 7, 2020, and August 10, 2020, the data that the cyberthieves claimed to have stolen had in fact been taken ("exfiltrated") from Defendant's computer systems.

43. The cyber-attack was specifically targeted at NWL, as the REvil ransomware operators posted public messages online indicating that they were contacted by a representative of a competitor company to compromise Defendant's networks, and that the competitor "offered us a good amount to satisfy our work in the National Western Life Infrastructure."[3]

[3] https://healthitsecurity.com/news/ransomware-hacking-groups-post-data-from-5-healthcare-entities (last accessed March 2, 2021)

44. The cyber-attack was also expressly designed and targeted to gain access to private and confidential data, including (among other things) the PII of Defendant's customers and clients. Evidence of this specific targeting of Private Information is the compromise and theft of the passports of the company CEO's family members. The REvil ransomware operators also sought payment directly from Defendant's clients whose Private Information was compromised and stolen, which is further evidence of the specific targeting.

45. Despite learning of the Cyber-Attack on or about August 15, 2020, NWL failed to make a timely and adequate response to the Cyber-Attack. Based upon the public postings from the REvil ransomware operators, files were still encrypted as late as August 23, 2020, and possibly later.

46. Moreover, letters written on Defendant's behalf indicate that while NWL alleged employed third-party investigators "immediately" "to determine the nature and scope" of the Cyber-Attack, it was not until on or about September 29, 2020, that "a third-party firm was engaged to programmatically and manually review the files at issue to identify all impacted individuals and the types of data associated with those individuals."[4]

47. NWL ultimately admitted to the Data Breach on or about December 21, 2020.

48. Despite learning of the Cyber-Attack on August 15, 2020, and despite the facts that A) the REvil ransomware operators were publicly posting customer data online in August 2020, and also B) were contacting NWL's affected customers directly in August 2020 seeking ransoms for stolen data, Defendant only began providing notice of the data breach beginning on or about January 14, 2021, in derogation of multiple state data breach notification statutes that require

[4] https://www.doj.nh.gov/consumer/security-breaches/documents/national-western-life-insurance-20210120.pdf (last accessed March 2, 2021)

notice as soon as possible, without unreasonable delay, or within a certain amount of time (typically 30 to 60 days after discovery of the data breach).

49. Compounding the problem, NWL's initial notice of data breach letters contained no information about the types of personal information impacted by the Cyber-Attack, and Defendant had to issue supplemental notices indicating that the stolen information contained Social Security numbers, life insurance or annuity policy numbers, and financial account information.

50. Outside experts have criticized companies that allowed their data to be breached, and who then delayed in notifying customers, downplaying the risk. Kate Borten, president of the privacy and security consulting firm The Marblehead Group, has stated (in the context of a healthcare related data breach):

> "Notification delay raises the risk of harm to patients . . . If patients are unaware that their information has been compromised, they cannot take protective steps."[5]

51. In the Notice Letter to Plaintiffs (attached hereto collectively as **Exhibit B**) and, upon information and belief, sent to the proposed classes, NWL admitted that:

> On August 15, 2020, NWL discovered a malware incident impacting certain company systems. We immediately launched an investigation, with the assistance of third-party investigators, to determine the nature and scope of this event. The investigation confirmed that certain data had been accessed and/or acquired by an unauthorized actor as a result of this event from August 7 to August 10, 2020. On December 21, 2020 we confirmed that personal information related to you was included in the impacted data.

52. NWL identified only the following actions it undertook to mitigate and remediate the harm caused by the Data Breach in the Notice Letter:

> As part of our ongoing commitment to the security of information, we notified federal law enforcement and we are reviewing and enhancing

[5] https://www.healthcareinfosecurity.com/notification-breach-affecting-219000-delayed-a-15986 (last accessed 2/22/2021)

> existing policies and procedures to reduce the likelihood of a similar future event.

Exs. B and C.

53. NWL recognized the substantial and high likelihood that Plaintiffs and the proposed classes' PII would be misused, instructing Plaintiffs and the proposed classes to:

> Please review the enclosed *Steps You can Take to Protect Your Information*, which contains information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against incidents of identify theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

Id. (parenthesis in the original).

54. NWL encouraged its policyholders and others who were notified of the Data Breach to contact the three credit-reporting bureaus to either place a "security freeze" or a "fraud alert" on their credit reports.

55. Based on the Notice of Data Breach letters they received (Exhibit B to this Amended Complaint), which informed Plaintiffs that their Private Information was removed from Defendant's network and computer systems, Plaintiffs believe their Private Information was stolen from NWL's networks (and subsequently sold) in the Cyber-Attack.

56. Further, the removal of the Private Information from NWL's system – information that included full names, dates of birth, and Social Security numbers (which are the keys to identity theft and fraud) -- demonstrates that this cyberattack was targeted.

B. PII is Stolen and Plaintiffs Face Significant and Imminent Risk of Identity Theft

57. Within days of the Data Breach, Data Breach victims' PII began being posted online.

58. On or about August 18, 2020, Cyble Vision, a digital Risk Management Platform, discovered that the unauthorized accessor of NWL's computer systems posted, on an online ransomware forum, that the accessor has stolen 656 gigabytes of NWL's confidential data. A copy of Cyble Vision's reporting is attached hereto as **Exhibit C.**

59. In the online post, the unauthorized accessor shared screenshots of a file that appears to contain credit card information of NWL's policyholders.

60. On or about August 23, 2020, the unauthorized user published another post sharing screenshots of NWL's policyholders' Social Security numbers, dates of birth, full name, dates of death, residence state, policy numbers, and policy termination date. *See* Ex. D.

61. Plaintiffs and members of the proposed classes have suffered injury from the misuse of their PII that can be directly traced to Defendant.

62. As a result of NWL's failure to prevent the Data Breach, Plaintiffs and the proposed classes have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII;

h. The continued risk to their PII, which remains in the possession of NWL and is subject to further breaches so long as NWL fails to undertake the appropriate measures to protect the PII in their possession.

63. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[6]

64. The value of Plaintiffs' and the proposed classes' PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

65. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

[6] *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN, (Dec. 15, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited February 9, 2021).

66. One such example of criminals using PII for profit is the development of "Fullz" packages. [7]

67. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

68. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed classes' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed classes, and it is reasonable for any trier of fact, including this Court or a jury, to find

[7] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), *available at* https://krebsonsecurity.com/tag/fullz/, (last visited February 10, 2020).

that Plaintiffs' and other members of the proposed classes' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

69. NWL disclosed the PII of Plaintiffs and members of the proposed classes for criminals to use in the conduct of criminal activity. Specifically, NWL opened up, disclosed, and exposed the PII of Plaintiffs and members of the proposed classes to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PII.

70. NWL's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and thousands of members of the proposed classes to unscrupulous operators, con artists and outright criminals.

71. NWL's failure to properly notify Plaintiffs and members of the proposed classes of the Data Breach exacerbated Plaintiffs' and members of the proposed classes' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

72. Upon information and belief, NWL knew the severity of the Data Breach but chose to downplay the Data Breach's impact. In the Notice Letter to Plaintiffs and members of the proposed classes, NWL did not disclose that the unauthorized accessor had been publicly disclosing Data Breach victims' PII online since August 2020 and that the unauthorized accessor had the ability to continually do so.

PLAINTIFFS' EXPERIENCES

73. Ms. Baldwin is a resident of and citizen of Missouri. Upon information and belief, Ms. Baldwin purchased a life insurance policy from NWL in 1994. Upon information and belief, the life insurance policy lapsed the same year.

74. As a condition of the life insurance policy purchase, NWL required Ms. Baldwin to provide the company with her PII.

75. Ms. Baldwin provided NWL her PII in order to purchase and receive the benefits of the life insurance policy.

76. On or about January 25, 2021, Ms. Baldwin received the Notice Letter from NWL, which informed her of the Data Breach and that she faced a substantial and significant risk of her PII being misused.

77. The Notice Letter did not inform Ms. Baldwin that the unauthorized accessor of NWL's computer systems had been posting Data Breach victims' PII online since August 2020.

78. As a result of the Data Breach, Ms. Baldwin expends a considerable time and effort monitoring her accounts to protect herself from additional identity theft. Ms. Baldwin fears for her personal financial security and is experiencing feelings of rage and anger, anxiety, sleep disruption, stress, fear, and physical pain. This goes far beyond allegations of mere worry or inconvenience; it is exactly sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

79. Mr. Dyrssen is a resident of and citizen of California. Upon information and belief, Mr. Dyrssen was an independent insurance agent licensed to sell NWL insurance policies for a period of time from 1993-1994.

80. As a condition of selling NWL insurance policies, NWL required Mr. Dyrssen to provide the company with his PII (which, at a minimum, included his name, address, phone number, date of birth, Social Security number, wife's name, and banking information).

81. Mr. Dyrssen provided NWL his PII in order to receive the benefits of being able to sell NWL policies as an independent agent.

82. A few days after January 25, 2021, Mr. Dyrssen received the Notice Letter from NWL, which informed him of the Data Breach and that he faced a substantial and significant risk of his PII being misused.

83. The Notice Letter did not inform Mr. Dyrssen that the unauthorized accessor of NWL's computer systems had been posting Data Breach victims' PII online since August 2020.

84. As a result of the Data Breach, Mr. Dyrssen expends a considerable time and effort monitoring his accounts to protect herself from additional identity theft. He receives 2-3 spam calls per day in addition to a few scam emails per week, all of which he attributes to the NWL data breach (because he was not receiving anywhere near the same amount of spam phone calls and emails until after the Data Breach occurred), and all of which cause him to expend considerable time to sift through for legitimacy. Since he received the Notice Letter, he has and continues to monitor his bank account twice per month for about 5-10 minutes each time.

85. Plaintiff Dyrssen has been placed at the imminent, immediate, and continuing risk of harm through the theft of his name and Social Security number, which are the keys to financial fraud.

CLASS ALLEGATIONS

86. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure Rule 23 on behalf of themselves and all members of the proposed class (the "Classes") as defined as:

> **National Class:** All persons in the United States whose data was compromised in the Data Breach announced on January 25, 2021 and who were mailed the Notice Letter.
>
> **Missouri Class:** All persons in Missouri whose data was compromised in the Data Breach announced on January 25, 2021 and who were mailed the Notice Letter.
>
> **California Class:** All persons in California whose data was compromised in the Data Breach announced on January 25, 2021 and who were mailed the Notice Letter.

87. The following people are excluded from the Classes: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

88. Plaintiff reserves the right to amend the definitions of the Classes or add a Class if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

89. Plaintiffs and members of the Classes satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 23.

90. **Numerosity:** The exact number of members of the Classes is unknown but, upon information and belief, the number exceeds 100,000, and individual joinder in this case is impracticable. Members of the Classes can be easily identified through Defendant's records and

objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

91. **Typicality**: Plaintiffs' claims are typical of the claims of other members of the Classes in that Plaintiffs, and the members of the Classes sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiffs and members of the Classes sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

92. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Classes and have retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Classes. Plaintiffs have no interests that conflict with, or are antagonistic to those of, the Classes, and Defendant has no defenses unique to Plaintiffs.

93. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

a. whether Defendant violated the laws asserted herein, including statutory privacy laws;

b. whether Defendant had a duty to use reasonable care to safeguard Plaintiffs' and members of the Classes' PII;

c. whether Defendant breached the duty to use reasonable care to safeguard members of the Classes' PII;

d. whether Defendant breached its contractual promises to safeguard Plaintiffs' and members of the Classes' PII;

e. whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

f. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and members of the Classes' PII from unauthorized release and disclosure;

g. whether proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiffs' and members of the Classes' PII from unauthorized release and disclosure;

h. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

i. whether Defendant's delay in informing Plaintiffs and members of the Classes of the Data Breach was unreasonable;

j. whether Defendant's method of informing Plaintiffs and other members of the Classes of the Data Breach was unreasonable;

k. whether Defendant's conduct was likely to deceive the public;

l. whether Defendant is liable for negligence or gross negligence;

m. whether Defendant's conduct, practices, statements, and representations about the Data Breach of the PII violated applicable state laws;

n. whether Plaintiffs and members of the Classes were injured as a proximate cause or result of the Data Breach;

o. whether Plaintiffs and members of the Classes were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiffs and members of the Classes;

p. whether Defendant's practices and representations related to the Data Breach breached implied warranties;

q. what the proper measure of damages is; and

r. whether Plaintiffs and members of the Classes are entitled to restitutionary, injunctive, declaratory, or other relief.

94. **Superiority:** This cause is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Classes will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendant's misconduct. Even if members of the Classes could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

95. A class action is therefore superior to induvial litigation because:

a. the amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

Count I
Negligence
(On Behalf of Plaintiffs, the National Class, the Missouri Class, and the California Class)

96. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

97. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain services, purchase life insurance products, or to sell NWL insurance policies as an independent agent.

98. Plaintiffs and members of the Classes entrusted their PII to Defendant. Defendant owed to Plaintiffs and other members of the Classes a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

99. Defendant owed a duty of care to Plaintiffs and members of the Classes because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Classes' PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

100. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

101. Defendant owed to Plaintiffs and members of the Classes a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Classes the scope, nature, and occurrence of the Data Breach. This duty is required and necessary in order for Plaintiffs and members of the Classes to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

102. Defendant owed these duties to Plaintiffs and members of the Classes because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and members of the Classes' personal

information and PII for insurance products purposes. Plaintiffs and members of the Classes were required to provide their personal information and PII to Defendant in order to receive insurance services from Defendant, and Defendant retained that information.

103. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

104. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and members of the Classes, and the importance of exercising reasonable care in handling it.

105. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and members of the Classes which actually and proximately caused the Data Breach and Plaintiffs' and members of the Classes' injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Classes, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Classes' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and members of the Classes have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

106. Defendant's breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs' and members of the Classes actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by

criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff Baldwin and the Missouri Class)

107. Plaintiff Baldwin and the Missouri Class members incorporate the above allegations as if fully set forth herein.

108. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff Baldwin's and the Missouri Class members' PII.

109. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, policyholders' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff Baldwin's and the Missouri Class members' sensitive PII.

110. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect its policyholders' PII and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to policyholders in the event of a breach, which ultimately came to pass.

111. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Missouri Class members.

112. Defendant had a duty to Plaintiff Baldwin and the Missouri Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff Baldwin's and the Missouri Classes' PII.

113. Defendant breached its respective duties to Plaintiff Baldwin and members of the Missouri Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff Baldwin's and the Missouri Class members' PII.

114. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

115. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff Baldwin and the Missouri Class, Plaintiff Baldwin and the members of the Missouri Class would not have been injured.

116. The injury and harm suffered by Plaintiff Baldwin and the Missouri Class members were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff Baldwin and members of the Missouri Class to suffer the foreseeable harms associated with the exposure of their PII.

117. Had Plaintiff Baldwin and members of the Missouri Class known that Defendant did not adequately protect policyholders' PII, Plaintiff Baldwin and members of the Missouri Class would not have entrusted Defendant with their PII.

118. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff Baldwin and the Missouri Class members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the insurance policies Plaintiff Baldwin and the Missouri Class members paid for that they would not have received had they known of Defendant's careless approach to cyber security; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

119.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff Baldwin and the Missouri Class)

120. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

121. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff Baldwin and the Missouri Class members by disclosing and exposing Plaintiff Baldwin's and the Missouri Class members' PII to enough people that it is reasonably likely those facts will become known to the public at large, including, without limitation, on the dark web and elsewhere.

122. Indeed, Plaintiff Baldwin and the Missouri Class members' PII was publicized to the public-at-large by virtue of the fact that the REvil Ransomware group publicized it online to attempt to extort a ransom from Defendant.

123. The disclosure of Missouri policyholders' full names, addresses, dates of birth, dates of death, Social Security numbers, policy numbers, policy termination dates, driver's license information, and passport information is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

124. Defendant has a special relationship with Plaintiff Baldwin and the Missouri Class members and Defendant's disclosure of PII is certain to embarrass them and offend their dignity. Defendant should appreciate that the cyber-criminals who stole the PII would further sell and disclose the PII as they are doing. That the original disclosure is devastating to Plaintiff Baldwin and the Missouri Class members, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large.

125. The tort of public disclosure of private facts is recognized in Missouri. *See Sullivan v. Pulitzer Broad. Co.*, 709 S.W.2d 475 (Mo. 1986). Plaintiff Baldwin's and the Missouri Class members' PII was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew or should have known that Plaintiff's and the Missouri Class members' PII is not a matter of legitimate public concern. As a direct and proximate result of Defendant's conduct, Plaintiff and Missouri Class members have been injured and are entitled to damages.

COUNT IV
Breach of Express/Implied Contractual Duty
(On Behalf of Plaintiff Baldwin, the National Class, and the Missouri Class)

126. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

127. Defendant offered to provide life insurance to Plaintiff Baldwin and members of the Classes in exchange for payment.

128. Defendant also required Plaintiff Baldwin and the members of the Classes to provide Defendant with their PII in order to purchase life insurance from Defendant.

129. In turn, and through its Privacy Policy, Defendant agreed it would not disclose PII it collects from customers to unauthorized persons. Defendant also promised to maintain safeguards to protect customers' PII.

130. Plaintiff Baldwin and the members of the Classes accepted Defendant's offer by providing PII to Defendant in applying for life insurance related products and services and then by paying for and receiving the same.

131. Implicit in the parties' agreement was that Defendant would provide Plaintiff Baldwin and members of the Classes with prompt and adequate notice of any and all unauthorized access and/or theft of their PII.

132. Plaintiff Baldwin and the members of the Classes would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

133. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Classes by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff Baldwin and members of the Classes by:

a. Failing to properly safeguard and protect Plaintiff Baldwin's and members of the Classes' PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

134. The damages sustained by Plaintiff Baldwin and members of the Classes as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

135. Plaintiff Baldwin and members of the Classes have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

136. The convent of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with

honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

137. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

138. Defendant failed to advise Plaintiff Baldwin and members of the Classes of the Data Breach promptly and sufficiently.

139. In these and other ways, Defendant violated its duty of good faith and fair dealing.

140. Plaintiff Baldwin and members of the Classes have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff Baldwin, the National Class, and Missouri Class)

141. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

142. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

143. Plaintiff Baldwin and members of the Classes conferred a monetary benefit upon Defendant in the form of monies paid for life insurance.

144. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff Baldwin and members of the Classes. Defendant also benefited from the receipt of Plaintiffs' and members of the Classes' PII, as this was used to facilitate payment and insurance claims.

145. As a result of Defendant's conduct, Plaintiff Baldwin and members of the Classes suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff Baldwin and members of the Classes paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

146. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that Plaintiffs and members of the Classes paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

147. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Classes all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VI
Violation of California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiff Dyrssen and the California Class)

148. Plaintiffs and the California Class members incorporate the above allegations as if fully set forth herein.

149. Plaintiff Dyrssen and members of the California Class are consumers who purchased products or services from Defendant primarily for personal, family, or household purposes.

150. Defendant's acts, practices, and omissions were done in the course of its business of marketing, offering for sale, and selling goods and services throughout the United States, including sales in the State of California.

151. Defendant violated Cal. Bus. and Prof. Code §17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the good and services provided to the California Class.

152. Defendant engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff Dyrssen's and Subclass members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff Dyrssen's and California Class members' PII in an unsecure electronic environment.

153. Defendant's conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices, including, among other things:

a. Failure to maintain adequate computer payment card processing systems and data security practices to safeguard customers' personal information;

b. Failure to disclose that its computer systems and data security practices were inadequate to safeguard customers' personal information from theft;

c. Failure to timely and accurately disclose the data breach to Plaintiff Dyrssen and the Class members.

154. The foregoing failures, acts and/or omissions were done in derogation of

standards set forth by the California Consumer Protection Act ("CCPA"), including but not limited to Cal. Civ. Code § 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the PII of Plaintiff Dyrssen and the California members; Federal Trade Commission ("FTC") Guidelines; and other readily available industry-wide resources that provide clear rules for the safeguarding of customers' PII in the State of California.

155. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and the California Class members' PII, and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Dyrssen and members of the California Class.

156. Defendant's unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff Dyrssen and the California Class members. They were likely to conceal the truth and deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff Dyrssen and the California Class members outweighed their utility, if any.

157. Defendant also engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the disclosure of the data breach to enact adequate privacy and security measures and protect California Class members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff Dyrssen and the California Class members. The harm these practices caused to Plaintiff Dyrssen and the California Class members

outweighed their utility, if any.

158. As a direct and proximate result of Defendant's unfair acts and practices, Plaintiff Dyrssen and the California Class members were injured and lost money or property, including but not limited to the loss of Plaintiff Dyrssen's and the California Class members' legally protected interest in the confidentiality and privacy of their PII, statutory and actual damages, and additional losses as further described herein, including but not limited to:

a. Actual theft of their personal information by criminals;

b. Actual or potential fraudulent charges on their payment card accounts, some of which were not reimbursed;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with the theft or fraudulent use of their financial accounts;

e. Loss of use of and access to some or all of their account funds and costs incurred as a result of being unable to access those funds;

f. Costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing, and seeking reimbursement for fraudulent charges, canceling and activating payment cards;

g. Purchasing products and services from Defendants that they would not have purchased had they known of Defendants' unfair practices;

h. Impairment to their credit scores and ability to borrow and/or obtain credit, and;

i. The continued risk to their personal information, which remains on Defendants' insufficiently secured computer systems.

159. Plaintiff Dyrssen and the California lass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, actual damages, statutory damages, restitution to Plaintiff and the Subclass members of money or property that the Defendants may have acquired by means of its unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and

injunctive or other equitable relief.

160. As a result of Defendant's violations, Plaintiff Dyrssen and members of the California Class are entitled to injunctive relief, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach, and;

h. Ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of personal information to third parties, as well as the steps its customers must take to protect themselves.

COUNT VII
Violation of California Consumer Privacy Act
Cal. Civ. Code § 1798.100, *et seq.*
(On Behalf of Plaintiff Dyrssen and the California Class)

161. Plaintiffs and the California Class members incorporate the above allegations as if fully set forth herein.

162. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff Dyrssen's and California Class members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff Dyrssen and California Class members.

163. As a direct and proximate result of Defendant's acts, Plaintiff Dyrssen's and the California Class members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure through NWL's computer systems and/or from the dark web, where hackers further disclosed NWL's customers' PII.

164. As a direct and proximate result of Defendant's acts, Plaintiff Dyrssen and the California Class members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

165. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard California Class members' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff Dyrssen and the California Subclass members.

166. NWL collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

167. Plaintiff Dyrssen and California Class members seek actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief,

attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court deems proper.

168. On March 2, 2021, Plaintiff Dyrssen provided written notice to Defendants identifying the specific provisions of this title he alleges they have violated. Within 30 days of Plaintiff Dyrssen's written notice, Defendant failed to "actually cure" their violations of Cal. Civ. Code § 1798.150(a). Plaintiff Dyrssen therefore seeks the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

COUNT VIII
Violation of California's Consumer Legal Remedies Act ("CLRA")
Cal. Civ. Code § 1750 *et seq*.
(On Behalf of Plaintiff Dyrssen and the California Class)

169. Plaintiffs and the California Class members incorporate the above allegations as if fully set forth herein.

170. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers. Defendants' acts, omissions, representations and practices as described herein fall within the CLRA because the design, development, and marketing of Defendants' insurance services are intended to and did result in sales of insurance services.

171. Plaintiff Dyrssen and the other California Class members are consumers within the meaning of Cal. Civ. Code §1761(d).

172. Defendant's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By omitting key information about the safety and security of the Network

and deceptively representing that it adequately maintained such information, Defendant violated the CLRA. Defendant had exclusive knowledge of undisclosed material facts, namely, that its Network was defective and/or unsecure, and withheld that knowledge from California Class members.

173. Defendant's acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of section 1770 the CLRA, which provides, in relevant part, that:

> a. The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
>
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . .
>
> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
>
> (9) Advertising goods or services with intent not to sell them as advertised.
>
> (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
>
> (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

174. For purposes of the CLRA, omissions are actionable along with representations.

175. Defendant stored California Class members' PII on its network. Defendant represented to California Class members that its network was secure and that their PII would remain private.

176. Defendant knew or should have known that it did not employ reasonable measures that would have kept California Class members' PII secure and prevented the loss or misuse of their PII. For example, Defendant failed to take reasonable steps to prevent the loss of PII through their servers through appropriate encryption and industry best practices.

177. Defendant's deceptive acts and business practices induced California Class members to provide PII, including Social Security numbers and driver's license numbers, for the purchase of goods and services. But for these deceptive acts and business practices, California Class members would not have purchased goods or services, or would not have paid the prices they paid for the goods or services.

178. Defendant's representations that it would secure and protect California Class members' PII in its possession were facts that reasonable persons could be expected to rely upon when deciding whether to purchase goods or services from Defendant.

179. California Class members were harmed as the result of Defendant's violations of the CLRA, because their PII was compromised, placing them at a greater risk of identity theft; they lost the unencumbered use of their PII; and their PII was disclosed to third parties without their consent.

180. California Class members suffered injury in fact and lost money or property as the result of Defendant's failure to secure their PII; the value of their PII was diminished as the result of Defendant's failure to secure their PII; and they have expended time and money to rectify or guard against further misuse of their PII.

181. Defendant's conduct alleged herein was oppressive, fraudulent, and/or malicious, thereby justifying an award of punitive damages.

182. As the result of Defendant's violations of the CLRA, Plaintiff Dyrssen, on behalf of himself, California Class members, and the general public of the State of California, seeks injunctive relief prohibiting Defendant from continuing these unlawful practices pursuant to California Civil Code § 1782(a)(2), and such other equitable relief, including restitution, and a declaration that Defendants' conduct violated the CLRA.

COUNT IX
Violation of the California Consumer Records Act ("CCRA")
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiff Dyrssen and the California Class)

183. Plaintiffs and the California Class members incorporate the above allegations as if fully set forth herein.

184. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

185. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

186. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

1. The name and contact information of the reporting person or business subject to this section;

2. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
3. If the information is possible to determine at the time the notice is provided, then any of the following:
    a. The date of the breach;
    b. The estimated date of the breach; or
    c. The date range within which the breach occurred.

187. The notification shall also include the date of the notice; whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; a general description of the breach incident, if that information is possible to determine at the time the notice is provided; and the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

188. The Data Breach described herein constituted a "breach of the security system" of NWL.

189. NWL unreasonably delayed informing Plaintiff Dyrssen and California Class Members about the Data Breach affecting their PII, after NWL knew the Data Breach had occurred.

190. Despite acknowledging that data thieves accessed Plaintiff Dyrssen's and the California Class Members' PII without authorization, NWL did not begin to notify affected individuals until January 25, 2021, over five months after the Data Breach occurred.

191. NWL failed to disclose to Plaintiff Dyrssen and California Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their

unencrypted, or not properly and securely encrypted, PII when NWL knew or reasonably believed such information had been compromised.

192. NWL's ongoing business interests gave NWL incentive to conceal the Data Breach from the public to ensure continued revenue.

193. Upon information and belief, no law enforcement agency instructed NWL that timely notification to Plaintiff Dyrssen and California Class Members would impede its investigation.

194. As a result of NWL's violation of Cal. Civ. Code § 1798.82, Plaintiff Dyrssen and California Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a fraud alert or credit freeze. These measures could have prevented some of the damages suffered by Plaintiffs and Class Members because their stolen information would have had less value to identity thieves.

195. As a result of NWL's violation of Cal. Civ. Code § 1798.82, Plaintiff Dyrssen and California Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

196. Plaintiff Dyrssen and Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff Dyrssen and California Class Members as alleged above and equitable relief.

197. NWL's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the NWL conducted with the intent on the part of NWL of depriving Plaintiff Dyrssen and California Class Members of "legal rights or otherwise causing injury." In addition, NWL 's misconduct as alleged herein is malice or

oppression under Cal. Civ. Code § 3294(c)(1) and (c)(2) in that it was despicable conduct carried on by NWL with a willful and conscious disregard of the rights or safety of Plaintiff Dyrssen and California Class Members and despicable conduct that has subjected Plaintiff Dyrssen and California Class Members to hardship in conscious disregard of their rights. As a result, Plaintiff Dyrssen and California Class Members are entitled to punitive damages against NWL under Cal. Civ. Code § 3294(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Classes, requests that the Court:

A. Certify this case as a class action on behalf of the Classes defined above, appoint Plaintiffs Mildred Baldwin and Douglas Dyrssen Sr. as the Class representatives, and appoint the undersigned as Class counsel;

B. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Classes;

C. Award injunctive relief as is necessary to protect the interests of Plaintiffs and the Classes;

D. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII;

E. Enter an award in favor of Plaintiffs and the Classes that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

F. Award restitution and damages to Plaintiffs and the Classes in an amount to be determined at trial;

G. Enter an award of attorneys' fees and costs, as allowed by law;

H. Enter an award of prejudgment and post-judgment interest, as provided by law;

I. Grant Plaintiffs and the Classes leave to amend this petition to conform to the evidence produced at trial; and

J. Grant such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: June 1, 2021.

Respectfully submitted,

/s/ Lynn A. Toops___

Lynn A. Toops
Lisa M. La Fornara*
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

Samuel J. Strauss*
TURKE & STRAUSS LLP
613 Williamson Street Suite 201
Madison, WI 53703
Tel: (608) 237-1775
Sam@turkestrauss.com

J. Gerard Stranch, IV*
Martin F. Schubert*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
martys@bsjfirm.com
peterj@bsjfirm.com

Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (202) 429-2290
gklinger@masonllp.com

*Motion for *pro hac vice* admission to be filed

Counsel for Plaintiff and the Proposed Class

Certificate of Filing

The undersigned hereby certifies that the foregoing Amended Complaint has been filed by using the Court's electronic case filing system thereby serving all parties of record on this 1st day of June, 2021.

/s/John F. Garvey